Some Thoughts on Networked Radicalization: Interview with Frank J. Cilluffo

Interviewed by John Whisenhunt, Editor

Editorial Abstract: Frank Cilluffo was a featured speaker at a US Northern Command sponsored Homeland Defense seminar, hosted by the JIOWC in June 2007. A noted strategist and US national policy advisor, Mr. Cilluffo shares his views on contemporary Islamic extremists, and their effective use of social networking. He further examines the current state of Western efforts to counter extremist messages, and a strategy for enhancing our actions in the cyber domain.

Frank J. Cilluffo
(George Washington University)

***IO Sphere**: We really appreciate the chance to talk with you today. Setting the stage, as we do with many of our guests, we note how the business of influence operations is too big and too complicated. Is there anyone you see that is doing that job well? Or that we could use as a model?*

Mr. Cilluffo: To be absolutely honest, I think the adversary is doing this job exceedingly well. They recognize the war is a war of ideas, and the battlefield is no longer the traditional one alone, but now in cyberspace. Their intent and objective is to influence, and get a message out that resonates, expands their ranks, energizes those who are already part of their organizations, and tries to justify and reaffirm—in my view—their aberrant attitudes. They've woven a very successful imaginary clash of civilizations by exploiting local political and economic grievances, some of which are very real, but then also peppering it with pieces and components that are absolutely false and manipulative. We need to be in the business of understanding that narrative, why is it resonating? Why is it sticking? Why is the 'brand' successful? We also need to recognize from a social networking standpoint why brands in general flourish and grow, and what makes them atrophy and die. We need to start looking at the second stage of issues. I think some of that is a shift in mindset, particularly in our own planning efforts, recognizing the need to move beyond tactics aimed at simply attacking their structures and toward those that are also attacking their strategy—aimed at what I consider to be a transnational insurgency underpinned by a global Salafi jihad. Here you have Al Qaeda 'Classic,' but you've also got the franchising of Al Qaeda, with their own indigenous objectives, but they tap into the larger movement. Perhaps it's best to think of it as groups that by and large think globally, but act locally.

Then you've got the third tier, where I think our homeland in particular needs to be concerned, and that's the 'leaderless' movement: those inspired by, but not directly part of any Al Qaeda organization. We need to understand that narrative… we've got to unpack it, and come up with a compelling counternarrative, that can get those on the brink—those potentially seduced by the jihadi Salafists—to actually counter that. This means our response cannot be government alone, you need someone who has credibility with the communities we're trying to influence. This has to some extent come from within. We need former jihadis coming out and denouncing terrorism, like Hassan Butt in the UK did in a *60 Minutes* interview, explaining how he felt duped by Al Qaeda. We need more of these sorts of messages, that are most effective. We need to remind people that the victims of terrorism are largely Muslim. We're not reminding them of Casablanca or Bali, or of Beslan, which killed how many children? We hear terrorists talk about their martyrs—well, we've had our martyrs, and it's time we actually recognize them, and not be afraid to show the world that bombing weddings in Jordan has consequences for the Jordanians, and for Muslims… killing children in schools, has consequences. The question needs to be asked: if, from their perspective, they're waging a war against the West, why have they killed so many Muslims? The Spanish government did this. They actually packaged a VHS tape showing another face of ETA [Basque separatist group].

We need to recognize that no single agency owns this mission—in fact it's beyond the federal government alone—we can't look at it from a centralized perspective. You can't defeat a networked adversary with a supercomputer, you have to defeat networks with other networks. We have to use all the elements of statecraft, and frankly we haven't done a good job marshaling all of those instruments. We have to win hearts and minds, remove terrorist masterminds, and offer opportunity for those who could be seduced by the terrorist message.

***IO Sphere**: That leads us into the next question. Careful use of language is something that comes up all the time in government forums like this. We tend to find that our expertise in cultural subtleties is scarce, and Western misuse of terms in the media works against us. Can you elaborate on that?*

Mr. Cilluffo: Sure. Words do matter, and they do have consequences. In many cases we're using the words they'd like us to use, because it further empowers and legitimizes their activities and their movement. Even the term 'jihad,' which refers either to inner struggle for righteous deeds or to external struggle against aggression and injustice in which strict rules of engagement concerning the protection of innocents apply, has been hijacked, because it's largely a defense measure that every Muslim engages in. Part of it is understanding the culture. We don't have nearly the same capacity in the military war colleges and in universities throughout the country as we had for the Soviet Union. Russian speakers were everywhere. Understanding the mind set was part and parcel in most national security and foreign affairs education activities. We're very slow to recognize and pick that up in the US. And part of that is we have to recognize some of the grievances are legitimate and recognize those, so we can unpack those that are absolutely 'off the charts.' So, our words do matter. I personally don't even use the term 'GWOT,' as it lets them feel that they are warriors and that what they are prosecuting is a legitimate and just war. I think they're really more like a bunch of thugs, and what they're doing is un-Islamic—they've actually corrupted and hijacked certain tenets of Islam, as corroborated by recent public opinion polls in several Muslim-majority countries by the Program on International Policy Attitudes. In Egypt, 77 percent of respondents believe that attacks on civilians are never justified; in Pakistan, it's 81 percent and in Indonesia, it's 84 percent of respondents. These are big numbers—most Muslims do not see this as legitimate. First and foremost we need the Islamic scholars—those that can use the Quran as an instrument—to demonstrate how it's being misused by those attempting to interpret it as a religious struggle.

***IO Sphere**: Let's go back to your comment on the 'network of networks.' You've written and spoken at length about cyber protection, and in your most recent US Senate testimony [May 2007] you talked about how our adversaries are effectively using the cyber domain for social networking. How well are our adversaries doing online?*

Mr. Cilluffo: I think you hit the right concept on the head: it's the social networking, the interaction between the physical and the cyber. It's the chat rooms, the dark corners where we need to be paying the most attention, not just the static Web pages. Those are important, but that's just propaganda. What we need is to get those people into the chat rooms that are well versed in the religion, and in some of the regional studies, to provide a counter narrative that will make sure we're not allowing the adversary to bring more into the extremist ranks, and energizing those ranks.

Historically they've used the Internet across the board, in support of tradecraft, for communications, fund raising, planning and coordination, training, operations security [OPSEC], information gathering and data mining, propaganda and misinformation dissemination, and radicalization and recruitment. But they really are networked, and we need to start doing some of the same. The 'killer application' of the Internet is *people*, and that it enables us to connect us globally—and reaffirm our views. You already have people who are predisposed to a particular set of views and issues-the Internet is great at that-in effect it 'Balkanizes' us. You and I can get all our news through an RSS [Really Simple Syndication] filter to justify our own thoughts—you name it. We are starting to lose context. You can drill deeper and deeper, continue to lose context, and people are going to actually think what they're doing is correct. Plus, there are two levels: those using it operationally, and those who could potentially become part of a movement. I think our emphasis needs to be on the second level.

***IO Sphere**: Recruitment versus command and control?*

Mr. Cilluffo: Recruitment and *enlistment*… self-enlistment… those that are inspired and seeking mutual support. But what is the life cycle? We recently brought together in a task force a group of multidenominational religious scholars, including Muslim religious scholars, behavioral scientists, as well as the national security community, to look at Internet-facilitated radicalization. We also did a study on prisoner radicalization, and what we were trying to get our arms around is the life cycle: what does it take to go from sympathizer, to activist, to indiscriminate violence? What are the points where we can intervene to peel that off? Sadly, I don't think there is a single profile—and I don't use that in the legal profiling sense, but in the behavioral sense. But you look at home grown cases in the UK, and the Internet has always played a significant role. For instance, in Casablanca, Morocco at an Internet café, an individual was told he could no longer monitor certain extremist Web sites, so he actually detonated himself at the café simply because he couldn't have access. So here you have someone who had no interaction with people; it was purely from the Internet. That certainly has implications. How often do we write in email things we would never say face to face? I try not to, being from a generation that still likes to speak to people! Too often people will blog things they wouldn't say to your face, and at this point in time, there's not much accountability. That's the biggest challenge: who's behind the 'clickity-clacks' on the keyboard? Though in the long run, I firmly believe that more information and greater transparency is the answer.

IO Sphere: We've already touched on what the West is doing about this. Would you like to expand on that?

Mr. Cilluffo: Two points on that. People ask "where are the 'moderate' Muslims' in countering extremism?" I don't like the term… I mean, what's a 'moderate Catholic?' I prefer simply 'Muslim'—those that are actually Islamic scholars. One thing many Americans don't fully appreciate is that Islam, or at least Sunni Islam, has no hierarchical clergy; there is no central leader such as the Pope in Catholicism. It's important to recognize that Muslim groups in America have stepped up, they've issued fatwas [official religious opinions] denouncing terrorism. A fatwa need not only be an edict justifying attacks. So they have been active, but no one—including the media—pays this any attention. Looking overseas, the Saudis are doing some innovative work—that's not to say all they're doing is on the positive side of the ledger. But they have what's called the Tranquility Program, where they go into the prisons and get jihadi senior leaders to denounce terrorism publicly on television. These sorts of people have credibility with those who can be seduced by the extremists. We have to find ways to facilitate 'exit ' so that sympathizers don't move to become activists.

***IO Sphere**: Where the spiritual component will validate that it's OK to get away from all that?*

Mr. Cilluffo: Absolutely. Also, the Moroccans are very active at using Muslim scholars for this sort of exit facilitation. In Britain, there is a community-based program called the Radical Middle Way, which is the project of a group of Islamic scholars who seek to discredit extremism through religion and promote a peaceful interpretation of Islam. While the UK government may not be completely happy with what they discuss, the group is vehemently opposed to terrorism as a tactic. Ultimately what we're talking about is providing a dream for the future and realistic opportunities. If you look in Europe, it's very different from the US, and you're largely seeing a generation that doesn't relate to their parents' generation, nor to their host country… I think almost every religion has this contemporary challenge. And there's a youth component… despite the cliché they're not all disenfranchised, unemployed youth. They feel they're underemployed. According to UK Home Office statistics, over 60 percent of those that have engaged in home grown terrorism have had graduate degrees.

***IO Sphere**: Let's shift a bit from the human 'wetware' aspect to the physical networking issue. A few years ago you warned the US leadership that we're too focused on lower level cyber protection… I believe you said "beeps and squeaks" level. How would you say we're doing nowadays?*

Mr. Cilluffo: Clearly there have been some across the board improvements. But I still feel the cyber domain is not treated at the same level as the kinetic and physical. In part it's because of the complexity, in part it's a generational issue. Many decision makers haven't grown up in that space, but many know how to exploit it even if they don't understand the nuts and bolts. While there have been many strategies, including a national strategy on protecting cyberspace, I still feel it's been a footnote in our overall planning efforts. That said, we've made some major improvements in protecting our physical infrastructure. I mean, a well placed bomb could be as debilitating, if not more so, than a cyber attack. To me, cyber is still to a great extent in the perception side, but it's also a force multiplier to enhance the lethality of physical attacks. I can't see a strict cyber attack—that doesn't mean someone won't do it—but many of Usama Bin Ladin's generation have their hands on AK-47s. But his next generation of children and nephews have their fingers on a computer mouse… we're seeing that. But I don't think they'll go entirely to cyber, rather they'll still see it as an enabler, to shape the battlefield for their physical actions.

Seeking 'true' Muslim voices. (Defense Link)

***IO Sphere**: So the hateful traditions endure, just with more high tech tools?*

Mr. Cilluffo: Most people feel they're motivated by hatred for the US, but that's an oversimplification. The far enemy, the US, is actually a convenient target to energize opposition to the near enemy. If they demonstrate they can attack the United States, they can get people energized to overturn the—from their perspective—'apostate' states in the Middle East. They need to have the 'bang' from their perspective, that they can actually do this. I feel the symbolic value of physical attacks is still so great at energizing their indigenous ranks to take on the—from their view—'apostate' states. That's a different perspective from many thoughtful analysts. While they exploit the activities in Iraq, I don't think that's their ultimate target: they still want to build, first and foremost, a Caliphate state spanning the Middle East. What I find somewhat surprising and disappointing is the unintended net effect of some of our policies has been to unite our adversaries, when I believe it's really time to divide and conquer. We have not tapped the disagreements to drive wedges between and among terrorist organizations.

My strategy would be something along the following: 1) isolate the military and operational planners from terrorist organizations; 2) isolate terrorist organizations from one another; 3) from that, isolate them from the larger movement;

and from that 4) isolate them from society writ large. Now, we can't take a one-size-fits-all approach, because it has different domestic dimensions depending on the host country. But we need to look at all the different dimensions that allow us to do that. We've barely tapped the cyber dimension of the battlefield, and [our adversaries] have been very good at that.

IO Sphere*: So when it comes to growing cyber expertise, who can we get to be technically and culturally astute? How do we recruit and entice people to come to work in this new battlefield of ideas?*

Mr. Cilluffo: Those are great questions. Not only do we have to find ways to recruit some of the best and brightest, I'm very concerned on the retention side. How do we keep people when they can be easily lured away at greater salaries in the private sector—they have less bureaucracy there, and they're empowered to do things. We have to find better people investments, and this is a leadership issue: how do we keep the best? How do we reward them, even if they make mistakes? How do we empower them, and get them to take calculated risks? Otherwise this has a chilling effect. So we have to work with academia and the universities to build the skill sets, that quite honestly may be better built outside of government. Recruiting has been on the uptick in places like the intelligence community, and that's a lot of young talent. The challenge now is that it generally takes five to seven years to go from entry level to be really effective as an analyst. And everyone is in the intelligence business now! It used to be the domain of a few entities, but now everyone is in the business and everyone is a customer. So you have a limited pool, and everyone is fishing, but it will still take us about five years to grow seasoned analysts. Then we have to retain them. In the CBRN [Chemical, Biological, Radiological, Nuclear] and cyber environments I'm not sure we're going to be able to stay cutting edge. And it's more than just the labs, it's in our day-to-day operations. It's not so much the recruiting as the retaining. This goes far beyond the traditional human resources functions: we also need to let them know they're making a difference. People on my staff at GW [George Washington University] could be making a lot more money, but they want to contribute—this is our generation's war. If you can't pay them a lot, you'd better be providing the 'psychic income' that acknowledges they're contributing and making a difference on important issues. While I can't think of a more noble cause than public service, I'm not sure our government structures have enabled and empowered that. We need to get beyond tinkering with boxes and 'org-charts' and invest in the people charged with the most awesome responsibilities our country faces. But if you look back, any successful leader has had to adapt. I'll leave you with a favorite quote I use with my students, from General [Dwight D.] Eisenhower: "In preparation for battle, I've often found plans to be useless, but planning to be indispensable."

IO Sphere*: You could almost say we're on a voyage of discovery versus following a plan?*

Mr. Cilluffo: Right, I think we're almost always on a voyage of discovery in this campaign. This part of the effort has us really 'going off road.'

IO Sphere*: Thank you again for taking the time from a very busy conference to speak with us.*

Mr. Cilluffo: It was great to be here John, thank you.